MariaDB Customer Data Processing Addendum

This Data Processing Addendum, including its appendices ("**DPA**") forms a part of, and is subject to, a written agreement or MariaDB order form ("**Agreement**") between a MariaDB legal entity ("**MariaDB**") and the customer ("**Customer**"), each as identified in the Agreement. It governs the processing of personal data by MariaDB on behalf of Customer for the provision of MariaDB database-as-a-service (MariaDB Cloud), cloud database administrator (CloudDBA), MariaDB Managed Database (MMD) and/or remote database administrator (Remote DBA) services ("**Services**").

All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

Customer enters into this DPA for itself and, as required by Applicable Data Protection Laws, on behalf of any of its Affiliates permitted to use the Services. For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and such Affiliates.

The parties agree as follows:

1. Definitions

1.1. "**Applicable Data Protection Laws**" means the European Data Protection Law and the CCPA.

1.2. "**CCPA**" means California Consumer Privacy Act of 2018 as amended by the California Privacy Rights Act of 2020 as amended, superseded or replaced on the effective date of this DPA.

1.3. "**Customer Personal Data**" means the personal data processed by MariaDB on behalf of Customer in connection with the provision of the Services, as further described in Annex A. In this DPA, any reference to "personal data" shall be understood to mean "Customer Personal Data" unless specified otherwise.

1.4. "**European Data Protection Law**" means (i) General Data Protection Regulation 2016/679 (GDPR); (ii) Directive 2002/58/EC; (iii) any applicable national implementations of (i) and (ii); (iv) Swiss Federal Act on Data Protection of 25 September 2020 (FADP); and (v) in respect of the United Kingdom, the Data Protection Act 2018; in each case, as may be amended, superseded or replaced on the effective date of this DPA.

1.5. "**Security Incident**" means any confirmed breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed by MariaDB and/or its Sub-processors in connection with the provision of the Services. "Security Incident" shall not include unsuccessful attempts or activities that do not compromise the security of personal data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

1.6. "**Standard Contractual Clauses**" or "**SCC**" means the Standard Contractual Clauses for the transfer of personal data to third countries pursuant to European Data Protection Law, annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021, as currently set out at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj.

1.7. "**UK Addendum**" means SCC as amended by the UK Addendum to the EU Standard Contractual Clauses, issued by the UK Information Commissioner's Office under version B1.0, as currently set out at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-data-transfer-agreement-and-guidance/.

1.8. "**Sub-processor**" means any processor engaged by MariaDB or its Affiliates to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA. Sub-processors may include third parties or MariaDB Affiliates but shall exclude any MariaDB employee, contractor or consultant.

1.9. The terms "**personal data**", "**controller**", "**processor**" and "**processing**" shall have the meaning given to them in European Data Protection Law and "**process**", "**processes**" and "**processed**" shall be interpreted accordingly. The terms "**consumer**", "**business**", "**business purpose**", "**sell**", "**service provider**" and "**personal information**" shall have the meaning given to them in the CCPA.

2. Scope and Applicability of this DPA

2.1. **Scope.** This DPA applies when MariaDB processes personal data protected by Applicable Data Protection Laws on Customer's behalf to provide the Services.

2.2. **Role of the Parties.** For the processing of personal data, Customer is a business or the controller (as applicable) and MariaDB is a service provider or the processor (as applicable). MariaDB will process personal data only on Customer's behalf as described in Annex A of this DPA. Both parties must comply with Applicable Data Protection Laws.

3. Processing of Customer Data

3.1. **Customer Instructions**. MariaDB will process personal data only for the purposes and in accordance with the documented instructions set forth in the Agreement, including this DPA. The Agreement and the Customer's use of the Services constitute the complete and final instructions. Any processing outside these instructions requires a prior written agreement. Without prejudice to Section 3.2 (Customer Responsibilities), MariaDB will notify Customer in writing if MariaDB becomes aware that a Customer instruction violates Applicable Data Protection Laws, unless prohibited by law.

3.2. **Customer Responsibilities**. Customer is responsible for the lawfulness of personal data processing under the Agreement. Customer represents and warrants it has provided and will continue to provide all notices and obtained and will continue to obtain all rights and consents required by Applicable Data Protection Laws for MariaDB to lawfully process personal data under this Agreement. Customer represents and warrants its processing instructions are lawful and that MariaDB's adherence to them will not cause MariaDB to breach any Applicable Data Protection Laws.

4. Sub-processing

4.1. **Authorized Sub-processors**. Customer acknowledges and agrees that MariaDB may engage Sub-processors to process personal data on Customer's behalf. A list of the Sub-processors currently engaged by MariaDB and authorized by Customer are available at MariaDB Online Trust Center (located at https://mariadb.com/trust) where Customer may elect to be notified of changes to MariaDB's Sub-processors. MariaDB will provide such notification at least 30 calendar days prior to any such changes.

5. Security and Audits

5.1. **Security Measures**. MariaDB shall implement and maintain appropriate technical and organizational security measures designed to protect personal data from Security Incidents and to preserve the security and confidentiality of personal data. Such measures will include, at a minimum, those measures described in Annex B of this DPA ("**Security Measures**"). MariaDB shall ensure that any person who is authorized by MariaDB to process personal data shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty). MariaDB conducts annual security reviews of its Sub-processors to ensure compliance with this DPA and applicable data protection laws.

5.2. **Updates to Security Measures**. MariaDB may update the Security Measures to reflect technical progress, provided such updates do not degrade the overall security of the Services.

5.3. **Customer Responsibilities**. Notwithstanding the above, Customer agrees that except as provided by this DPA, Customer is responsible for its secure use of the Services, including securing its account authentication credentials, selecting appropriately narrow access controls and address whitelists, protecting the security of personal data during transit to and from the Services, and taking any appropriate steps to securely encrypt or back up any personal data processed in connection with the Services. Customer shall implement and maintain appropriate technical and organizational security measures designed to protect personal data from Security Incidents and to preserve the security and confidentiality of personal data while in its dominion and control.

5.4. **Security Incident Response**. Upon becoming aware of a Security Incident, MariaDB shall notify Customer without undue delay and shall provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Customer.

5.5. **Security Audits**. To demonstrate its compliance with this DPA, upon Customer's written request (no more than once annually), MariaDB will make available its most recent third-party audit reports or certifications (e.g., SOC 2, ISO 27001) and will provide written responses to reasonable information requests and security questionnaires. Notwithstanding the foregoing, Customer may also exercise such audit right in the event Customer is expressly requested or required to provide this information to a data protection authority, or MariaDB has experienced a Security Incident, or on another reasonably similar basis.

6. International Transfers

6.1. **Processing Locations.** Customer acknowledges and agrees that MariaDB may transfer and process personal data to and in the United States and other locations where MariaDB, its Affiliates, or Sub-processors operate. MariaDB will ensure all such transfers comply with Applicable Data Protection Laws and this DPA.

6.2. **Transfers from the European Economic Area.** Where the transfer of personal data is from the European Economic Area (EEA), the parties agree to be bound by the SCC, Module Two (Controller to Processor) and Module Three (Processor to Processor). The SCC are hereby incorporated by reference.

6.3. **Transfers from the United Kingdom.** Where the transfer of personal data is from the United Kingdom, the parties agree to be bound by the UK Addendum, Module Two (Controller to Processor) and Module Three (Processor to Processor). The UK Addendum is hereby incorporated by reference.

6.4. **Implementation of the SCC and UK Addendum**. For the purposes of the SCC and UK Addendum: (1) MariaDB is a “data importer” and Customer is the “data exporter” (notwithstanding that Customer may itself be an entity located outside the EEA or the UK); (2) the module two (controller to processor) terms shall apply to the extent Customer is a controller of personal data and MariaDB is a processor, and the module three (processor to processor) terms shall apply to the extent Customer is a processor of personal data; (3) Clause 7 shall not apply, (4) Clause 9, Option 2 of the applicable module of the SCC shall apply and MariaDB may engage Sub-processors as described in Section 4 of this DPA; (5) in Clause 11, the optional language shall be deleted; (6) the audits described in Clauses 8.3 and 8.9 of the SCC shall be carried out as set out in and subject to the requirements of Section 5.5 of this DPA; (7) pursuant to Clauses 8.5 and 16(d) of the SCC, upon termination of this DPA, personal data will be returned or destroyed in accordance with Section 7 of this DPA; (8) in Clause 17, Option 1 shall apply and the SCC shall be governed by Irish law; (9) in Clause 18(b), disputes shall be resolved before the courts of Ireland; (10) Annex A and Annex B of this DPA shall replace Annexes I and II of the SCC and Annexes 1A, 1B and II of the UK Addendum. If and to the extent the SCC conflicts with any provision of this DPA regarding the transfer of personal data from Customer to MariaDB, the SCC shall prevail to the extent of such conflict.

6.5. **EU-U.S. Data Privacy Framework.** For transfers of personal data to the United States from the European Economic Area (**EEA**), its Member States, and Switzerland, MariaDB may annually certify its adherence to the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and the Swiss-U.S. Data Privacy Framework (collectively, the “**Data Privacy Framework**” or “**DPF**”). If the DPF is not available or is invalidated for a transfer, that transfer will be subject to the SCC and applicable laws as set out in this DPA.

7. Deletion or Return of Personal Data

7.1. On termination of the Agreement and at Customer's written request, MariaDB will delete or return all personal data in its control. This does not apply to data MariaDB must retain by law or to data on backup systems. MariaDB will isolate and protect such retained data from further processing and delete it according to its standard practices.

8. Rights of Data Subjects and Cooperation

8.1. **Data Subject Requests**. If Customer cannot access personal data through the Services to respond to a data subject request, MariaDB will provide reasonable assistance at Customer’s sole expense. If MariaDB receives a request directly, it will not respond without Customer's prior authorization, unless legally required. If legally required to respond, MariaDB will promptly notify Customer and provide a copy of the request, unless prohibited by law.

9. Jurisdiction Specific Terms

9.1. **Europe.** To the extent the personal data is subject to European Data Protection Laws, the following terms shall apply in addition to the terms in the remainder of this DPA:

9.1.1. **Sub-processor Obligations**. MariaDB shall: (i) enter into a written agreement with each Sub-processor imposing data protection terms that require the Sub-processor to protect personal data to the standard required by applicable European Data Protection Law and this DPA; and (ii) remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause MariaDB to breach any of its obligations under this DPA.

9.1.2. **Objections to Sub-processors**. Customer may object in writing to MariaDB’s appointment of a new Sub-processor on reasonable grounds relating to data protection (e.g. if making personal data available to the Sub-processor would violate applicable European Data Protection Law or weaken the protections for such personal data) by notifying MariaDB promptly in writing within 30 calendar days of receiving notification from

MariaDB in accordance with Section 4.1. Such notice shall explain the reasonable grounds for the objection and the parties shall discuss Customer's concerns in good faith with a view to commercially reasonable resolution.

9.1.3. **Resolution of Objections**. If the parties cannot find a commercially reasonable solution to Customer's objection, MariaDB may propose a price increase to accommodate the changes required to resolve the objection. If the parties do not agree on the price change within 30 days, MariaDB may terminate the Agreement with written notice.

9.1.4. **Adequate level of protection**. To the extent that MariaDB processes (or causes to be processed) any personal data protected by European Data Protection Laws in a third country not recognized as providing an adequate level of protection for personal data (as described in applicable European Data Protection Laws), MariaDB agrees to abide by and process personal data in compliance with the SCC, which are incorporated in full by reference and form an integral part of this DPA.

9.1.5. **Data Protection Impact Assessment**. To the extent MariaDB is required under applicable European Data Protection Law, MariaDB shall provide reasonably requested information regarding MariaDB's processing of personal data under the Agreement to enable the Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by law.

9.2. **California**. To the extent the personal data is subject to the CCPA, the parties agree that Customer is a business and that it appoints MariaDB as its service provider and/or contractor to process personal information on behalf of the Customer for the business purposes specified in Annex A. MariaDB shall not: (a) "sell" or "share" personal information (as defined by the CCPA); (b) retain, use or disclose personal information for any purpose other than for the specific business purposes specified in the Agreement and its Annexes, or as otherwise permitted by CCPA; (c) retain, use or disclose personal information outside of the direct business relationship between Customer and MariaDB, except where required by law; (d) combine the personal information received from or on behalf of Customer with personal information that it receives from other sources, except as permitted under the CCPA. Notwithstanding the above, MariaDB may de-identify or aggregate personal information in the course of providing the Services. MariaDB shall provide reasonable assistance to Customer in facilitating compliance with consumer rights requests under applicable U.S. State Privacy Laws.

10. Miscellaneous

10.1. Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict.

10.2. The total aggregate liability of each party and its Affiliates arising out of or related to this DPA, including the SCC, whether in contract, tort, or under any other theory of liability, is subject to the limitations and exclusions of liability set out in the Agreement. For the avoidance of doubt, in no event shall the total aggregate liability of either party or its Affiliates under this DPA exceed the maximum aggregate monetary liability of that party or its Affiliates as set out in the Agreement.

10.3. This DPA may be executed in counterparts, each of which will be deemed an original, but all of which together will constitute one and the same instrument.

10.4. If any part of this DPA is found to be invalid or unenforceable, it will be deemed deleted, but the rest of the DPA will remain in effect.

10.5. This DPA shall be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by European Data Protection Law.

IN WITNESS WHEREOF, the parties have caused this DPA to be executed by their authorized representatives and this DPA shall be effective on the date both parties sign this DPA.

Customer		**MariaDB**	
By:	_____	By:	_____
Name:	_____	Name:	_____
Title:	_____	Title:	_____
Date:	_____	Date:	_____

ANNEX A
DATA PROCESSING DESCRIPTION

A. List of Parties

Data exporter(s). Customer and Affiliates (if any) permitted to use the Services.

Data importer(s). MariaDB and its Affiliates.

B. Description of Transfer

Categories of data subjects whose personal data is transferred. The data subjects are determined by Customer and may include the Customer's employees, clients, suppliers, business partners and end-users.

Categories of personal data transferred. Customer data uploaded by Customer to the Services or otherwise made available to MariaDB in accordance with the Agreement is determined and controlled by Customer. The personal data may include:

- *Personal Details*: Names, job titles, addresses, email addresses, phone numbers, IP addresses.
- *Financial Data*: Transaction IDs, payment statuses, or other financial records.
- *Authentication Data*: Usernames or account identifiers.
- *Geolocation Data*: Location information and coordinates.

Sensitive data transferred (if applicable). The parties do not intend for any special category data to be processed under the Agreement.

The frequency of the transfer. The parties intend a continuous transfer of personal data as instructed by Customer under the Agreement.

Nature of the processing. Delivery of the MariaDB Cloud, CloudDBA, MMD and/or Remote DBA services, and to provide related technical support as agreed with Customer.

Purpose(s) of the data transfer and further processing. The personal data may be subject to the following basic processing activities:

- processing to provide the Service in accordance with the Agreement.
- processing to perform any steps necessary for the performance of the Agreement.
- processing initiated by Customer in its use of the Service.
- processing to comply with other reasonable instructions provided by Customer (e.g. via email or support tickets) that are consistent with the terms of this Agreement.

The period for which the personal data will be retained. The duration of the data processing under this DPA is until the termination of the Agreement in accordance with its terms plus the period from the expiry of the Agreement until deletion of personal data by MariaDB in accordance with the terms of the Agreement.

C. Competent Supervisory Authority

Data Protection Commission (DPC) in Ireland.

ANNEX B
DESCRIPTION OF THE TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

MariaDB implements the following technical and organizational security measures to protect personal data it processes.

Physical Access Control

MariaDB has implemented, or has ensured that its Sub-processors have implemented, specific measures to prevent unauthorized persons from gaining physical access to the premises, buildings or rooms where data processing systems are located which process personal data. These controls include:

- Restricted access to specified, authorized individuals, including to data centres/rooms where servers are located;
- Video surveillance and alarm devices for such access areas;

System Access Control

MariaDB has implemented controls to prevent data processing systems from being used without authorization. These controls include:

- Password protections for all systems processing personal data (including remote access);
- Access authentication which includes:
    - Individual user passwords;
    - dedicated user IDs for every individual;
    - multi-factor authentication for access;
- Access granted to authorized personnel only;
- Access granted is the minimum required to perform the individual's function/role;
- A password policy that prohibits the sharing of passwords and outlines the processes to be followed after a password has been disclosed;
- Passwords always stored in encrypted form;
- A procedure to deactivate user accounts (including administrator permissions) when a user leaves MariaDB or a specific function/role;
- Access logs;
- Review of such access logs for any security incidents.

Data Access Control

MariaDB has implemented controls to ensure persons entitled to use a data processing system shall gain access only to the data to which they have a right of access, and personal data must not be read, copied, modified or removed without authorization in the course of processing. These include:

- Restriction of file and program access to a “need-to-know” basis;
- Prevention of use/installation of unauthorized hardware and/or software;
- Rules for the safe and permanent destruction of data that are no longer required;
- Access granted to authorized personnel only;
- Access granted is the minimum required to perform the individual's function/role.

Data Transmission Control

MariaDB has implemented controls to ensure personal data cannot be read, copied, modified, or removed without authorization during transmission or while in storage, and to make it possible to establish to whom personal data was transferred.

Data Entry Control

MariaDB has controls in place to examine and establish whether and by whom personal data have been entered into data processing systems, modified or removed. These controls include:

- Access logs showing administrators' and users' activities;
- Restriction on modification of personal data to authorized personnel only.

Job Control

MariaDB has implemented controls to ensure personal data is processed in the performance of a service for the Customer. These include ensuring:

- Processing of personal data is only for contractual performance;
- Staff members and contractors comply with written instructions and contracts;
- Personal data is always logically separated so that, in each step of the processing, the Customer from whom personal data originated can be identified.

Availability Control

MariaDB implements the following controls to protect personal data against disclosure, accidental or unauthorized destruction or loss:

- Backup copies stored in protected environments;
- Contingency plans and/or business recovery strategies;
- Restriction on use of data only for purposes MariaDB is contracted to perform;
- Firewalls to prevent unauthorized access to systems and services.

Organizational Requirements

MariaDB implements technical and organizational measures to avoid the accidental mixing of personal data, including:

- A designated individual responsible for data protection;
- Written commitments from employees to maintain confidentiality;
- Staff training on data privacy and security;
- Security incident response procedures and staff training where applicable.